___ FILED ___ ENTERED
___ LOGGED ____ RECEIVED

4:00 pm, Oct 08 2020
AT BALTIMORE
CLERK, U.S. DISTRICRT COURT
DISTRICT OF MARYLAND
BY _____Deputy

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No.: 1:20-mj-2379 TMD
	)	
The Domain Name	)	
AllianceFunding-Covid19.com	)	
("SUBJECT DOMAIN NAME")	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Michael McFarland, being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant is a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI) (formerly known as the United States Customs Service and hereinafter referred to as HSI). I am assigned to the Office of the Special Agent in Charge, Baltimore, Maryland, and I have been employed by HSI since 2002. I am currently assigned to the Transnational Cyber Crimes Team.

2. Prior to my employment with HSI as a special agent, I served as a police officer in Louisiana as a patrol officer and as a military police officer with the U.S. Air Force for a total of seven years. In addition to my primary employment, I currently hold the rank of Lieutenant Colonel as a commissioned officer in the U.S. Air Force (U.S. Air Force Reserves) assigned to Air Force Office of Special Investigations (AFOSI), as the Augmentee to the Commander of a detachment located oversees. Prior to AFOSI, I was an Army Aviator and piloted UH-60 Black Hawk aircraft. I have deployed and served in Saudi Arabia, Afghanistan, and Iraq, and currently have over 30 years of honorable service within the Armed Services.

3. I have conducted and participated in numerous investigations of criminal activity, including, but not limited to, narcotic and firearms smuggling, intellectual property crimes,

counter proliferation/illegal exportations, cyber-crimes, and crimes against children to include child pornography and sex tourism. Your affiant has also completed the sixteen-week Basic Training Course known as Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. Furthermore, your affiant has received training from the Federal Bureau of Investigations, in the area of computer crime investigations, U.S. Customs Service Cyber Crimes Internet course at FLETC and DOD Defense Cyber Crimes Center.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. As set forth below, there is probable cause to believe that the domain **AllianceFunding-Covid19.com**, ("SUBJECT DOMAIN NAME") is property used, or intended to be used, to commit or facilitate violations of Title 18, U.S.C. § 1343 (wire fraud) and other federal felony offenses, such as 18 U.S.C. § 1030 (fraud and related activity in connection with computers) (collectively, the "SUBJECT OFFENSES"), and subject to seizure and forfeiture pursuant to Title 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2), and 1030(i). I make this affidavit for a warrant to seize the property described in Attachment A, specifically, the SUBJECT DOMAIN NAME.

6. The procedure by which the government will seize the SUBJECT DOMAIN NAME is described in Attachment A hereto and below.

BACKGROUND ON DOMAIN NAMES

7. Based on my training, experience, and experience and information learned from

others, I am aware of the following:

8. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

9. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

10. Domain Name System: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and is the web server.

11. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol ("IP") addresses.

12. Registry: For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

13. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

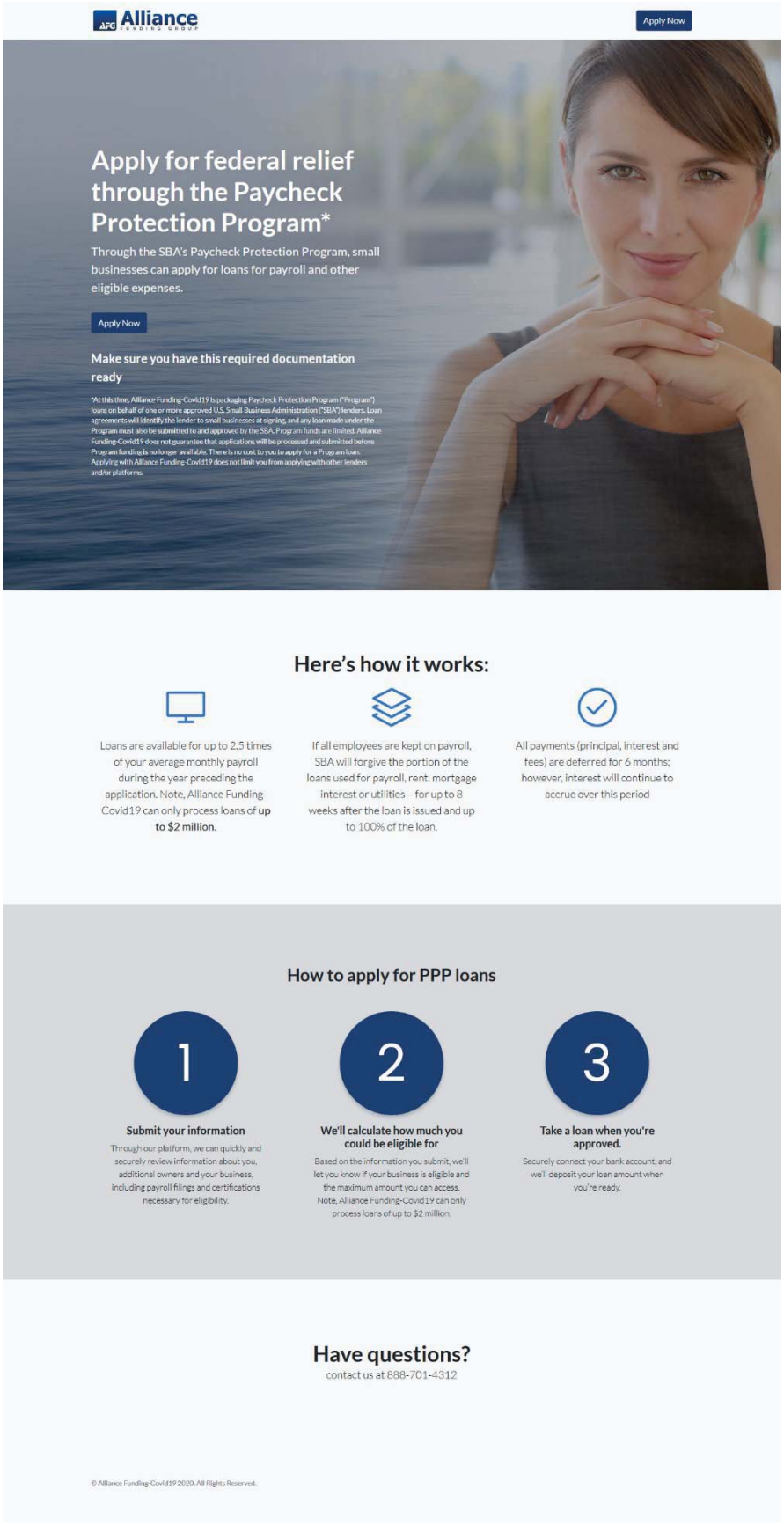
14. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

CASE BACKGROUND

15. On March 13, 2020, the President of the United States declared a national emergency due to the COVID-19 pandemic.

16. On or about August 18, 2020, during an ongoing proactive operation targeting suspicious publicly reachable websites HSI Cyber Crimes Center (C3) located a website named AllianceFunding-Covid19.com (the "SUBJECT DOMAIN NAME").

17. On August 18, 2020, C3 conducted a review of the SUBJECT DOMAIN NAME content online which displayed the name and logos for Bank Number 1, a financial funding company located in California which specializes in equipment leasing, financing, working capital, and Small Business Administration (SBA) loans. The SUBJECT DOMAIN NAME home page stated; "Apply for the federal relief though the Paycheck Protection Program (PPP), small businesses can apply for loans for payroll and other eligible expenses." In addition, the home page specifically mentions AllianceFunding-Covid19 is packaging the PPP loans on behalf of one or more approved US SBA lenders. Furthermore, the homepage provides details on how to apply for PPP loans in three steps. Submit your information, secondly, AllianceFunding-Covid19 will calculate how much the applicant is eligible for, and the last step is to securely connect the applicant's bank account and the SUBJECT DOMAIN NAME will deposit the loan amount. This process begins by clicking the "Apply Now" button which is located on the home page and provides a link to multiple webpages where potential applicants can provide personal information. Some examples of personal information requested which would be needed for a SBA loan include, name, date of birth, home address, phone number, tax ID number, wage or net earnings, and social security number. Below is a picture of the website:


Alliance
FUNDING GROUP
Apply Now
Apply for federal relief through the Paycheck Protection Program*
Through the SBA's Paycheck Protection Program, small businesses can apply for loans for payroll and other eligible expenses.
Apply Now
Make sure you have this required documentation ready
*At this time, Alliance Funding-Covid19 is packaging Paycheck Protection Program ("Program") loans on behalf of one or more approved U.S. Small Business Administration ("SBA") lenders. Loan agreements will identify the lender to small businesses at signing, and any loan made under the Program must also be submitted to and approved by the SBA. Program funds are limited. Alliance Funding-Covid19 does not guarantee that applications will be processed and submitted before Program funding is no longer available. There is no cost to you to apply for a Program loan. Applying with Alliance Funding-Covid19 does not limit you from applying with other lenders and/or platforms.
Here's how it works:
Loans are available for up to 2.5 times of your average monthly payroll during the year preceding the application. Note, Alliance Funding-Covid19 can only process loans of up to $2 million.
If all employees are kept on payroll, SBA will forgive the portion of the loans used for payroll, rent, mortgage interest or utilities – for up to 8 weeks after the loan is issued and up to 100% of the loan.
All payments (principal, interest and fees) are deferred for 6 months; however, interest will continue to accrue over this period
How to apply for PPP loans
1
Submit your information
Through our platform, we can quickly and securely review information about you, additional owners and your business, including payroll filings and certifications necessary for eligibility.
2
We'll calculate how much you could be eligible for
Based on the information you submit, we'll let you know if your business is eligible and the maximum amount you can access. Note, Alliance Funding-Covid19 can only process loans of up to $2 million.
3
Take a loan when you're approved.
Securely connect your bank account, and we'll deposit your loan amount when you're ready.
Have questions?
contact us at 888-701-4312
© Alliance Funding-Covid19 2020. All Rights Reserved.

18. On or about August 18, 2020, C3 contacted the Vice President for Portfolio Servicing at Bank Number 1 and confirmed Bank Number 1 provided SBA loans, however they did not create or authorize the SUBJECT DOMAIN NAME, AllianceFunding-Covid19.com. The authentic domain name for Bank Number 1 is similar to the SUBJECT DOMAIN NAME. Bank Number 1 requested HSI investigate and prevent the website using the SUBJECT DOMAIN NAME from further operation to prevent any fraud and victimization. The Bank Number 1 representative reiterated that Bank Number 1 did not authorize anyone to use their business name or logos outside of their control and specifically requested the domain name be removed.

19. Upon further review of the SUBJECT DOMAIN NAME, C3 Special Agents also noted the graphics were strikingly similar as Bank Number 1's authentic domain name, to include logos, formatting, and color schemes. The phone number listed on the SUBJECT DOMAIN NAME was 888-701-4312. Your affiant called the number listed on the website from the District of Maryland and it appears to be a calling servicing center that only allows for a voice message to be recorded. Open source reveals this phone number has had past fraud allegations. In addition, unlike other authentic web pages, the web pages for the SUBJECT DOMAIN NAME did not provide any other contact methods other than the phone number listed above such as email or a business address. Furthermore, there are no other links such as "About, Contact, Privacy Policy, and Terms of Use" as a few examples which are typical for authentic business web pages.

20. On August 19, 2020, C3 was notified by GoDaddy LLC., that the SUBJECT DOMAIN NAME had its services suspended for violations of GoDaddy's Terms of Service. This was based on C3's information which was passed to GoDaddy LLC., for their review and

course of action.

21. On August 23, 2020, a "Domain Whois Record" search indicated the SUBJECT DOMAIN NAME was created on April 12, 2020, resolved to the IP Address of 34.69.36.118, and the registrar was listed as GoDaddy.com LLC. In addition, the registrant's information for the SUBJECT DOMAIN NAME was left blank, possibly to avoid their identity from being discovered. Some examples of items left blank include, name, address, and phone number.

22. On August 23, 2020, your affiant utilized an online tool known as Domaintools.com. Domaintools is a resource utilized by law enforcement to conduct whois searches but the resource can also provide useful information regarding the potential risks of specific domain names. DomainTools Risk Score predicts the risk level and likely threats associated with a domain that has not yet been observed in malicious activities by analyzing intrinsic properties of the domain that are observable as soon as the domain is registered. A search of the SUBJECT DOMAIN NAME indicated an overall risk of 98 out of 100 and listed the largest threat as "Phishing." In addition, other threats included Malware (41 of 100), and spam (56 of 100).

23. On August 23, 2020, a search of the ICANN[1] Registry Listings, indicated the registry for ".com" domains is: VeriSign, Inc., located at 12061 Bluemont Way, Reston, VA 20190. Their email was listed as info@verisign-grs.com and phone number as 703-948-3200.

24. Your affiant knows from my training, education, and experience that criminals who operate websites and use targeted domain names such as the SUBJECT DOMAIN NAME

[1] The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management.

often conceal their identity when registering their domain names by redacting personal identifiers, to avoid being tracked by victims or law enforcement. In addition, your affiant believes, based on training, education, and experience, that this website was setup for the purpose of collecting customers' personal identification in order to use that information for nefarious purposes such as fraud, which could include phishing attacks and/or deployment of malware.

THE SUBJECT DOMAIN NAME

25. As described above, the SUBJECT DOMAIN NAME was used by unknown subjects to commit a violation of Title 18, United States Code, Sections 1343 and 1030.

26. A search of publicly available WHOIS domain name registration records revealed that the SUBJECT DOMAIN NAME was registered on or about April 12, 2020 through the registrar GoDaddy.com Inc., which has its headquarters at Scottsdale, Arizona. The publicly available WHOIS database does not list any of the registrant's information other than California and the US for state and country. GoDaddy.com Inc. is an entity that allows website owners to keep their contact details private during the domain name registration process.

27. As discussed in paragraph 23, the top-level domain for the SUBJECT DOMAIN NAME is VeriSign, Inc., 12061 Bluemont Way, Reston, VA 20190 and currently manages all ".com" domains.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

28. Title 18, United States Code, Section 1030(i)(1) provides, in relevant part, that upon conviction for an offence under Section 1030, the Court shall order the forfeiture of the defendant's "interest in any personal property that was used or intended to be used to commit or

facilitate the commission" of any violation of Section 1030.[2]

29. The procedures set forth in Title 21, United States Code, Section 853 govern the seizure and disposition of property as well as the conduct of judicial and administrative forfeiture proceedings under Title 18, United States Code, Sections 982(b) and 1030(i)(2). Title 21, United States Code, Section 853(f) authorizes the issuance of a criminal seizure warrant and provides, in relevant part, that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture. Similarly, Title 18, United States Code, Section 981(b), authorizes seizure of property subject to civil forfeiture, again, based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3), permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and the execution of that seizure warrant in any district in which the property is found.

30. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the SUBJECT DOMAIN NAME for forfeiture. By seizing the SUBJECT DOMAIN NAME and redirecting it to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the SUBJECT DOMAIN NAME will prevent third parties from continuing to access

---

[2] Title 18, United States Code, Section 1030(i)(2) allows, in relevant part, for forfeiture of proceeds traceable to a violation of Section 1030. Title 18, United States Code, Section 981(a)(1)(C), provides, in relevant part, that any property that constitutes proceeds of violations of Title 18, United States Code, Section 1343 and 1030 are subject to civil forfeiture by the United States. Finally, Title 18, United States Code, Section 982(a)(2) likewise provides, in relevant part, that any property that constitutes proceeds of violations of Title 18, United States Code, Sections 1343 and 1030 are subject to criminal forfeiture by the United States.

AllianceFunding-Covid19.com in its present form.

31. Venue for civil forfeitures lies (1) in any district in which any of the acts or omissions giving rise to the forfeiture occurred pursuant to Title 28, United States Code, Section 1355(b)(1)(A) (1); (2) in the district in which such property is found, pursuant to Title 28, United States Code, Section 1395(b); or (3) in any district where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought pursuant to Title 18, United States Code, Section 981(h).

32. As set forth above, there is probable cause to believe that the SUBJECT DOMAIN NAME is subject to civil and criminal forfeiture because it was used in the commission of violations of the SUBJECT OFFENSES. Specifically, the SUBJECT DOMAIN NAME was involved in wire fraud and enabled computer fraud related activity in connection with computers, which were conducted in violation of Title 18, United States Code, Section 1343 and 1030.

SEIZURE PROCEDURE

33. As detailed in Attachment A, upon execution of the seizure warrant, VeriSign, Inc., the registry for the ".com" top-level domain (the SUBJECT REGISTRY), headquartered at 12061 Bluemont Way, Reston, VA 20190, shall be directed to restrain and lock the SUBJECT DOMAIN NAME pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAME to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAME cannot be made absent court order or, if forfeited to the United States, without prior consultation with Homeland Security Investigations or DOJ.

34. In addition, upon seizure of the SUBJECT DOMAIN NAME by Homeland Security Investigations, VeriSign Inc., will be directed to associate the SUBJECT DOMAIN

NAME to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the SUBJECT DOMAIN NAME will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

.

.

CONCLUSION

35. For the foregoing reasons, I submit that there is probable cause to believe that the SUBJECT DOMAIN NAME is used in and/or intended to be used in facilitating and/or committing the SUBJECT OFFENSES. Accordingly, the SUBJECT DOMAIN NAME is subject to forfeiture to the United States pursuant to 21 U.S.C. § 853, 18 U.S.C. §§ 1343 and 1030, and I respectfully request that the Court issue a seizure warrant for SUBJECT DOMAIN NAME.

36. Because the warrant will be served on VeriSign Inc., which controls the SUBJECT DOMAIN NAME, thereafter, at a time convenient to it, will transfer control of the SUBJECT DOMAIN NAME to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

MICHAEL T MCFARLAND II

Digitally signed by MICHAEL T MCFARLAND II
Date: 2020.09.15 11:46:11 -07'00'

Michael T. McFarland
Special Agent, Homeland Security Investigations

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 22 day of Sept., 2020

HONORABLE THOMAS M. DIGIROLAMO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

With respect to "AllianceFunding-Covid19.com" ("SUBJECT DOMAIN NAME"), VeriSign, Inc., who is the domain registry for the SUBJECT DOMAIN NAME, shall take the following actions to effectuate the seizure of the SUBJECT DOMAIN NAME:

1) Take all reasonable measures to redirect the SUBJECT DOMAIN NAME to substitute servers at the direction of Department of Homeland Security - Homeland Security Investigations, by associating the SUBJECT DOMAIN NAME to the following authoritative name-server(s) or **by redirecting traffic to the SUBJECT DOMAIN NAME to the following IP addresses**:
    (a) Ns1.seizedservers.com (IP address 66.212.148.117);
    (b) Ns2. seizedservers.com (IP address 66.212.148.118); and/or
    (c) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar.
2) Prevent any further modification to, or transfer of, the SUBJECT DOMAIN NAME pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAME to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAME cannot be made absent court order or, if forfeited to the United States, without prior consultation with the Department of Homeland Security.
3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
5) The Government will display a notice on the website to which the SUBJECT DOMAIN

NAME will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> "The domain for AllianceFunding-Covid19.com has been seized by the Department of Homeland Security - Homeland Security Investigations and the Baltimore County Police Department in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, and 1030 by the United States District Court for the District of Maryland as part of a law enforcement action by the United States Department of Justice."

ATTACHMENT B

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") and the domain name registrars based in the United States listed in Section III ("Subject Registrars"). The Subject Registry will be directed, for the domain names listed in Section IV ("Subject Domain Names") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the domain name pending transfer of all rights, title, and interest in the Subject Domain Name to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall point the Subject Domain Names to the IPR Center's Domain Names ns1.seizedservers.com (IP address 66.212.148.117) and ns2.seizedservers.com (IP address 66.212.148.118) and at which the Government will display a web page with the following notice:

> *"The domain for AllianceFunding-Covid19.com has been seized by the Department of Homeland Security - Homeland Security Investigations and the Baltimore County Police Department in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, and 1030 by the United States District Court for the District of Maryland as part of a law enforcement action by the United States Department of Justice."*

C. Upon seizure of the Subject Domain Names, the Subject Registry will take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the subject domain names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with the Department of Homeland Security.

D. Upon seizure of the Subject Domain Names, the Subject Registrars based in the United States shall contact the registrant of the Subject Domain Name and provide them notice of the seizure along with the following contact information:

(a)	Name:	Homeland Security Investigations National Intellectual Property Rights Coordination Center
(b)	Address:	2451 Crystal Drive, Suite 200 Arlington, VA 20598-5105
	Country:	USA
(c)	Telephone:	1-866-IPR-2060 (477-2060)
(d)	Email:	IPRCenter@dhs.gov
(e)	Fax:	703-603-3872

II. Subject Registry

VeriSign, Inc.,
12061 Bluemont Way
Reston, VA 20190

III. Subject Registrars based in the U.S.

Godaddy.com, Inc.
14455 N. Hayden Road, Suite 226
Scottsdale, AZ 85260

IV. Subject Domain Name(s): AllianceFunding-Covid19.com